



Gaining Visibility and Control of “Inside Out” SSL Web Sessions

EXECUTIVE SUMMARY

Web applications (and their derivatives – IM, P2P, Web Services) continue to comprise the overwhelming majority of new applications being deployed across today's distributed enterprises. Much of the new growth in Web application development is focused on business-critical applications. Furthermore, many of these applications and related components are hosted by 3rd parties or accessed over public infrastructure. Not surprising, the criticality and confidentiality of Internet-accessible applications has caused organizations to rely more heavily on SSL encryption. Unfortunately, as organizations increase the amount of encrypted traffic coming in to the enterprise, IT becomes increasingly "blind" to their traffic – particularly SSL interactions between enterprise users and external applications. This blind spot raises many security, control, and performance questions. Can threats move within these tunnels? Can users subvert enterprise control? Can encrypted applications be accelerated for optimized performance?

If an organization were to adopt a solution to resolve these issues, it would need to understand native SSL traffic flowing to external applications, be operationally affordable, not impede business (neither performance nor privacy), and be extensible and adaptable.

Unfortunately, past technology efforts to resolve these issues for unencrypted traffic have proved inadequate – none can "see" the encrypted traffic. While SSL offload or SSL VPN technologies can help organizations manage SSL traffic for applications that they control, there has not been a practical solution for "inside-out SSL." In other words, traditional security and networking solutions cannot effectively protect users inside the corporate network from safely accessing applications and information outside the corporate network (e.g., Salesforce.com, employee benefits providers, and the wide variety of non-business-related applications their employees use).

Blue Coat's new SSL proxy functionality enables organizations to extend the power of the intelligent and secure proxy appliances to all SSL traffic – both internal and external. Because this is a proxy, traffic is terminated – enabling unprecedented visibility and context – and then reinitiated, according to the policies set by IT. Termination by a proxy is the only way to gain visibility and control of SSL communications. It provides a critical control point for protection (against viruses, worms, spyware, and phishing), policy (manage the who, what, where, when, and how of user/application interaction), and performance (cache, compress, and prioritize traffic). This new functionality is part of Blue Coat's market-leading proxy appliance, ProxySG, which means that organizations benefit from the deployability of the Blue Coat solution – using an appliance form factor, single operating system, and single enterprise management platform – all with a track record of thousands of enterprise deployments.

Organizations need to take care in deploying SSL proxy functionality. Enterprises should ensure that their acceptable use policies incorporate the appropriate language, and that they take advantage of ProxySG's granular controls to mitigate any potential privacy concerns.

Control.

SSL TRAFFIC ON THE RISE

Organizations continue to implement Web model applications (Web apps, “Web 2.0,” XML, Web services, etc.). This has comprised the overwhelming majority of new application development for the last several years. As enterprises become more comfortable with Web technologies, and more adept at deploying (or buying) them quickly, Web technologies are being used for business-critical applications. With that criticality, however, security issues associated with Web technologies become more important. Indeed, to a large degree, enterprise Web applications must be deployed with the assumption that they will be accessed over public infrastructure (i.e., the Internet) – whether that is because the application is hosted by a third party, or simply because users are accessing the application that is based outside the enterprise. This assumption dictates that most enterprise Web applications are typically accessed over an encrypted channel – Secure Sockets Layer (SSL) to increase confidentiality and integrity. In fact, some leading edge organizations have adopted an all-SSL approach for their networks in an effort to protect the privacy of all their communications. Additionally, enterprise users are relying on SSL to access partner applications (e.g., suppliers, researchers)

Finally, consumers continue to conduct more of their personal business online – which further adds to the growth in SSL traffic. All of these dynamics contribute to massive growth in SSL-encrypted traffic – where enterprises are experiencing double the amount of SSL traffic they had a year ago (7-10% growing to 14-20%), and expecting SSL to comprise 30% of Web traffic next year. (source: Blue Coat ProxySG customer logs and projections).

IT IS BLIND TO ENCRYPTED TRAFFIC

SSL encryption was designed to create a trusted class of Web traffic – when the little padlock shows up in a browser, the traffic is deemed “secure.” This confidentiality has enabled businesses and consumers to take advantage of “anywhere, anytime, any user” encrypted connection to drive tremendous commercial exploitation of the Web. There is, however, a downside: encryption, the very thing that keeps prying eyes from SSL traffic, also makes it nearly impossible to see, understand, or manage that traffic. Indeed, in most organizations, port 443 (the designated port for SSL traffic) is completely unscrutinized – traffic freely and blindly flows in and out of the enterprise. This raises

three sets of issues: first, IT lacks any control over this traffic; second, IT has no ability to protect itself from threats flowing in the encrypted traffic stream; and third, IT cannot prioritize and accelerate encrypted traffic – some of which may be mission-critical.

Lack of Policy Control

Driven by security, regulatory, and liability concerns, a growing number of organizations are attempting to manage enterprise Web traffic (witness the growth in URL and content filtering). The growth in SSL traffic, however, means that IT’s ability to manage and control user/application interaction is declining. So the IT budget spent on URL filtering is dwindling in effectiveness, as SSL communication offers an easy way to circumvent corporate policy. Additionally, rogue applications like Skype, peer-to-peer file sharing applications, and IM all use port 443 (some encrypt, some do not) since they know that IT has no ability to examine such traffic.

Lack of Protection

Information security threats increasingly use SSL to propagate, hide, and increase effectiveness. Some of these threats (viruses, worms, Trojans) use SSL inadvertently – via Web mail (e.g., Gmail over HTTPS – which does not have virus scanning) or collaborative extranet applications.

Threats can also encrypt with SSL deliberately – some examples:

- “Secured” phishing, where the attack is performed over SSL to escape detection, and to increase the appearance of authenticity
- “Secured” spyware or “researchware” (e.g., Marketscore), where all user traffic is run through Marketscore’s servers via SSL
- Guardster, s-tunnel, JAP and other anonymizing services designed to circumvent controls.
- Viruses and worms that leverage encryption have been predicted, and remain on the horizon

For most organizations, the information security group is chartered to manage risk – which they cannot do if a significant percentage of user/application communications is invisible to them.

Lack of Performance

Given the importance of many of the business applications using SSL, it is obvious that SSL-enabled enterprise applications should be afforded the highest performance. They are typically applications that need acceleration technologies (caching, compression) most. Unfortunately, because of the encrypted nature of this user/application interaction, acceleration is impossible with today's dedicated network acceleration gear. If the traffic is invisible, it cannot be compressed, cached, or accelerated in any fashion. As a result, performance of critical applications may suffer.

WHAT DOES THE IDEAL SOLUTION LOOK LIKE?

For organizations that elect to address this "blind spot," what is the right solution? First, the solution must understand and control native SSL traffic. Second, business performance and processes cannot be impeded. Third, nobody wants to pay more for the solution than the problem costs – so it must be operationally affordable. Fourth, the solution cannot be a dead end, single capability that requires more hardware for every feature – it must be extensible and adaptable.

Natively understand and control SSL – who, what, where, when, how?

Any solution deployed for this purpose should be able to fully understand SSL – not just a few parameters of its packet stream. Fundamentally, this means the ability to grasp, and govern user-application interaction – including who (e.g., actual end user), what (e.g., application type, actual app), where (e.g., where is the user, where is the application coming from), when (e.g., priority, time of day, quota), and how (e.g., protocol, method, user agent). Given the encrypted nature of SSL traffic, there is only one way to understand all of these attributes – a solution must terminate SSL traffic and become part of the tunnel.

Doesn't Impede Business

The solution cannot impede the flow of business. There are several requirements that can be extrapolated from this statement. First, given the criticality of (some) SSL traffic, the solution cannot introduce significant latency into the enterprise network – up to very high (100s of Mbps) throughputs. Second, given the sensitive nature of SSL, the solution should have the flexibility of being able to pass-

through certain known, appropriate traffic, while examining and controlling other traffic. This granularity should extend to any caching functionality as well. Finally, logging and auditing must be flexible and thorough, to prevent any opportunity for abuse.

Operationally Affordable

Any solution should be manageable across a large enterprise. This translates to something that is easily deployed in large numbers, and furthermore, can be efficiently managed across those large numbers. Typically, this means that the solution is ideally delivered in an appliance form factor, involving as simple a deployment as possible. Additionally, large enterprises will require centralized enterprise management capabilities – deployment, configuration, monitoring, and reporting.

Extensible and Adaptable

Enterprises are always trying to increase predictability – in cost, in vendor management, and in integration and operations. The last thing most organizations want is yet another single-purpose box. Generally, organizations want best-of-breed functionality, yet integrated into a solution that covers a class of problems.

CAN CURRENT TECHNOLOGIES ALLEVIATE THE PROBLEM?

Unfortunately, existing technologies mostly attempt to inspect the few unencrypted elements around the interaction (port, IP address), but are hardly able to understand the nature of the traffic, let alone that of the user-application interaction. Routers, firewalls, and intrusion detection/prevention systems cannot inspect encrypted traffic. Similarly, URL filtering databases can help a bit in that they can categorize IP addresses, but operate from the same limitations – they can't see the nature of the traffic or the interaction – because the traffic remains encrypted, so even the hostname is typically obscured. URL filtering databases are becoming more popular, but alone their effectiveness is waning with the growth in SSL traffic.

HTTP proxies are often used to increase control over an organization's Web traffic. Due to the nature of proxies (i.e., they terminate the protocols that they proxy), they offer a higher degree of control than simple URL filtering databases. Even so, simply proxying HTTP doesn't help with the SSL issue. SSL-offload and SSL VPN solutions have often been

Control.

placed in front of application servers to help scale Web servers making heavy use of SSL or, in the case of SSL VPN, to provide a cost-effective mobile remote access solution. Unfortunately, these solutions aid IT only in managing SSL that they already control – they cannot help organizations control “inside-out” SSL traffic from external sites.

THE POWER OF THE PROXY

Because a proxy is an active device (i.e., it terminates traffic), it acts as both the server to the client, and the client to the server. Thus, it has a native understanding of both the user and the application. For many organizations, users will only connect to the Internet via a proxy – because of the control it affords an enterprise. Because a proxy terminates connections, it offers a critically important control point for policy, performance, and protection of all Web-enabled user and application interactions.

Blue Coat's ProxySG is the leading secure proxy appliance, offering enterprises “the power of the proxy” in a broad range of sizes. Blue Coat extends that leadership by offering SSL proxy functionality on its market-leading proxy appliance.

Protection

Blue Coat's protection capabilities include components built into ProxySG that guard against spyware, phishing, and pharming via ProxySG's native understanding of applications, content, protocols, and users. Furthermore, Blue Coat's ProxyAV appliances integrate with ProxySG to scan Web traffic for threats, without negatively impacting application performance.

Blue Coat's protection extends from HTTP-based applications to any application or exploit that uses Web protocols – including IM-based threats and exploits that target specific browsers.

Policy

Because ProxySG terminates and reissues all supported application traffic (HTTP, SSL, FTP, streaming, P2P, IM, telnet, DNS, etc.), it has native understanding of application and user interactions. This also enables fine-grained, policy-based control – ProxySG has over 500 different triggers and actions it can automatically apply to govern interactions between applications and users – managing who, what, where, when, and how. Some examples include:

- **Who:** ProxySG integrates with all major authentication systems and user stores, so identifying a user and mapping his credentials back to a group, locating the role he plays in the organization, and the access rights afforded to him are possible – all from within the proxy appliance.
- **What:** ProxySG understands the different types of applications running over the Web – e.g., static and dynamic Web pages, instant messaging, peer-to-peer, email, Web mail, FTP. ProxySG also understands which individual application, and what kind of transaction (protocol, method, etc.) is underway.
- **Where:** ProxySG's ability to run the broadest possible set of filtering databases enables organizations to exert control over where applications come from – both from types of servers and applications, and from specific sources.
- **When:** ProxySG's controls extend to time – enterprises can enforce policies about when users can get to a specific application and how much they can do, as well as enforce priority over different types of application traffic (e.g., Web mail can only take up 5% of bandwidth).
- **How:** Finally, ProxySG can govern how users and applications interact – which user agents (clients), which protocols and methods, and what modes of interaction (e.g., no javascript).

All of the above controls incorporate a variety of different actions – including the ability to allow the transaction, advise or coach the user, deny the interaction, strip offending content, modify to comply with policy, and throttle application traffic by any of the aforementioned variables.

Performance

Again, because a proxy acts as both client and server, and has full visibility and context of the user-application interaction, it is uniquely suited to apply acceleration techniques – including bandwidth management (i.e., limit the unimportant traffic so business-critical traffic flows unimpeded), compression, and a variety of caching techniques.

BLUE COAT SSL PROXY

Blue Coat has introduced additional functionality to ProxySG – an SSL proxy. In addition to proxying encrypted traffic, there are several SSL-specific features that enable organizations to exert more flexible control over encrypted traffic. They are described below in the context of the solution criteria laid out earlier in this paper.

Natively Understand and Control SSL

ProxySG's SSL proxy functionality terminates SSL traffic. It can exert policy control at the initiation of the SSL session (i.e., on client connect, and on server response) and throughout the session – because there are two separate SSL connections: one between the client and the proxy, and another between the proxy and the server – see Figure 1. This enables all of the proxy controls laid out in the previous section, but also some SSL specific controls. First, ProxySG can make gateway trust decisions – meaning that organizations can decide whether or not they will accept secure connections from servers with questionable certificate (e.g., the certificate is out of date, or issued by an untrusted party, or doesn't match the server name), instead of trusting their users to make that determination. This has tremendous anti-phishing benefits – most of the servers used in phishing and pharming attacks depend on users blithely clicking “yes” to certificate warnings. Second, ProxySG's SSL proxy functionality can proxy SSL, hand off any HTTPS to the HTTP proxy, and manage traffic tunneling through SSL (typically rogue applications like Skype, Peer-to-peer, or IM) differently – deciding whether or not to pass that traffic – which has significant benefits for security groups trying to manage vulnerability-prone consumer applications.

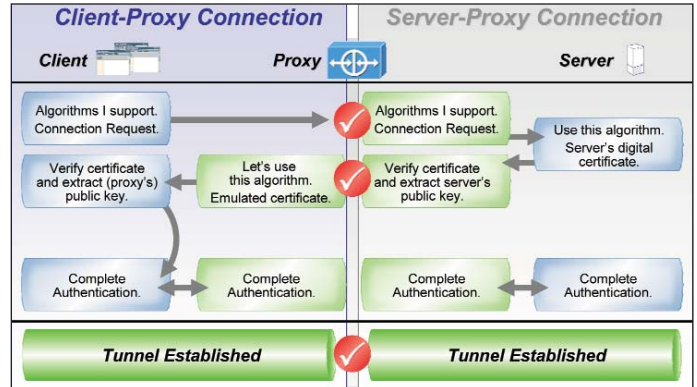


Figure 1 – ProxySG provides critical check points during SSL session initiation and management, including checking policies on users accessing external Web content, checking certificates used in the SSL connection, and ensuring inbound/outbound information does not compromise security or compliance policies.

Will Not Impede Business

Blue Coat customers have deployed ProxySG to manage Web traffic in some of the largest organizations in the world. For some customers who deploy ProxySG for security and control reasons, the surprise is that application performance improves as a result of the integrated acceleration techniques (compression and caching). Correctly sized, ProxySG will handle any size network, and accelerate overall session performance. The other important aspect to note is the flexibility of the SSL proxy functionality – organizations can, based on a variety of criteria (e.g., user, application, source):

- Pass-through SSL traffic untouched,
- Make some initial judgments about where the traffic is coming from and going to, then pass it through, or
- Fully proxy the SSL connection.

These three options are represented in the three diagrams in Figure 2.

Control.

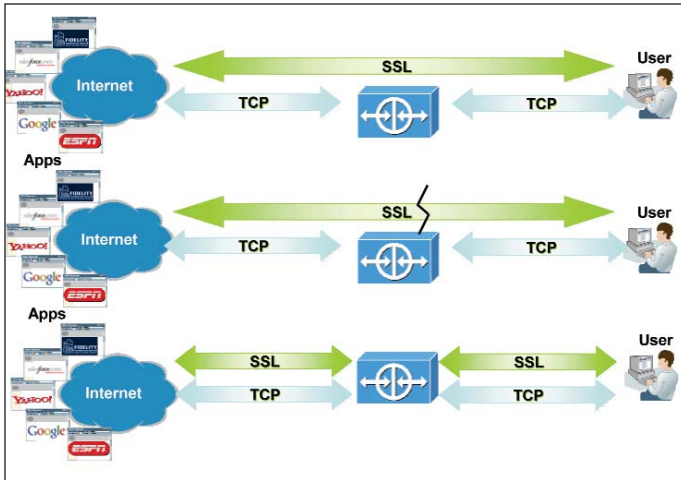


Figure 2 – Blue Coat enables IT organizations to apply varying levels of SSL proxy management, from simply passing through traffic to full proxy enabling policy-based SSL control.

In the latter two of the above scenarios, organizations can also warn end-users of what is going on (e.g., a splash page that lets users know that some monitoring is going on, and remind them of the acceptable use policy). This flexibility extends to caching, logging, and administrative functions as well. Using ProxySG's SSL proxy capabilities, organizations can be selective about what they cache – perhaps only caching certain elements that do not contain sensitive data (e.g. GIFs and JPEGs). Similarly, logging can be equally selective, and organizations can send the logs off to a secure server to ensure auditability.

Deployability and Management

As stated above, ProxySG is deployed in many of the world's largest enterprises. This is not a coincidence: ProxySG is an appliance, and has one operating system (SGOS) – regardless of which models an organization chooses. SGOS has grown organically, not through mergers and acquisitions. Furthermore, Blue Coat's Director and Reporter products enable organizations to manage and report across an enterprise of many ProxySGs.

Extensible and Adaptable

Blue Coat proxy appliances are a foundation for making the Web work for business. ProxySG's capabilities solve the gamut of Web security and performance issues, and are not a "one-off," single-purpose solution. Whether

threats materialize as spyware, phishing, viruses, worms, productivity-sapping rogue applications, or liability-inducing inappropriate content, ProxySG prevents them from entering enterprises – all while accelerating legitimate application traffic.

CONCLUSION

SSL traffic is growing into a significant amount of enterprise network traffic. For "inside-out" SSL – interactions between users inside the enterprise and applications outside it, this is a significant blind spot for IT. IT is unable to secure, control, or accelerate this traffic. Blue Coat's new SSL proxy removes IT's blinders, enabling organizations to establish a critical control point for policy, performance, and protection of users and applications using SSL. While enterprises should update acceptable use policies, Blue Coat's solution affords the appropriate flexibility and controls to mitigate any potential privacy concerns within the enterprise.



650 Almanor Ave.
Sunnyvale, CA 94085
www.bluecoat.com

1.866.30.BCOAT
408.220.2200 Direct
408.220.2250 Fax

Copyright ©2005 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use, Blue Coat is a registered trademark of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners. Version 1.0

Blue Coat Systems provides secure proxy appliances that control user communications over the Web. Blue Coat ProxySG appliances integrate advanced proxy functionality with security services such as content filtering, instant messaging control and Web virus scanning – without impacting network performance. With more than 3,000 customers and over 14,000 appliances shipped worldwide, Blue Coat is trusted by many of the world's most influential organizations to ensure a safe and productive Web environment. Blue Coat is headquartered in Sunnyvale, California, and can be reached at 408.220.2200 or www.bluecoat.com.